







في





ظافر ناصر السبيعي

الجزء الأول

DAFER181@HOTMAIL.COM

مقدمة

كونـي خبير حاسب الآلـي كان الناس يأتون ألـي ، ليسلونـي عن كيفية حماية الحاسب من الفيروس وذلك لعلمهم آن ذرة وقاية خير من قنطار علاج وكذلك كيف التعامل مع الحاسب ، وكنت أرد بكل ما كنت أعلمه فـي حينـه.

أما ألان فأريد أن أجيب عن هذا السؤال فـي هذه الصفحات بما أدركه اليوم وهو ليس موجوداً فـي الكتاب التقليدي من الحفظ وسترجع المحفوظ

نـعم هو الخيال كيف يعمل تفكيرك مفتاح صغير

وأنت معلم لنفسك

الصورةعن الف كلمة



الشكل الدائري في الحاسب:



الشكل الدائري هو الشكل الوحيد الذي قطره ثابت

الشكل الدائري ليس له حواف حادة

الشكل الدائري صعب الكسر

الشكل الدائري مناسب لاستدارة مع السرعة

الشكل الدائري يوزع الثقل بعدالة على جميع الاتجاهات

ذاكره البطاريه:





بطاريات الليثيوم Lithium ion فلها أداء عظيم ويمكن أن تترك من غير استعمال للفترات الطويلة بدون أن تخسر شحنها، عندما اشتريت اول هاتف نقال اخبرني صديقي انه من الافضل ان يتم تفريغ البطاريات قبل أعاده شحنها مره أخرى وسبب ذلك يعرف بما يسمى بذاكره البطارية وذلك بتفريغ شحن البطارية (او استهلاكها) بشكل كامل ثم أعاده شحنها مره أخرى إلى الحد الأعلى وهذا يعطيك أفضل أداء وأعلى سعه للبطارية.

بخلاف ذلك لو أنت قمت بشحن البطارية وهي نصف ممتلئة إلى إن تمتلئ ستتعامل البطارية مع نقطه نصف الامتلاء كما لو كانت هي نقطه فراغ الشحن(اى إن هذه ألنقطه هي نقطه التفريغ) وهذا يقلل كفاءة بطارية وأيضا سعتها

لا ينصح بأستخدم أكثر من مضاد فيروسات واحد ، وكذلك بالنسبة للجدار الناري



لما سيحدث من التعارض وكل برنامج فيروسات سيعتبر البرنامج الآخر هو عبارة عن فيروسات ، وأنبه على أن برنامج مضاد الفيروسات يختلف عن مضاد ملفات التجسس كا (الأدوير) أو (السباي وير) وغيرها ، فلا بأس باستخدام أكثر من برنامج مضاد تجسس بل هذا هو الأفضل.

شبكات الحاسب



شبكة الكومبيوتر هي مجموعة من أجهزة الكومبيوتر PCs والأجهزة الأخرى المتصلة بعضها البعض بواسطة كوابل . الشبكة مختلفة في حجمها فهي تبدأ من جهازين على أقل تقدير وتنتهي بملايين الأجهزة . الشبكة الموجودة ضمن منطقة مساحة محددة لا تتجاوز المكتب أو المبنى الواحد تدعى (LAN) Local Area Networkingوهي شبكة تضم مجموعة من التجهيزات مثل كومبيوترات PCs وطابعات ومخدمات Serversوموزعات Hubs وهي كما قلت تعطي مساحة

المشاركه..(Sharing)



فأنت عندما تُوصل الحاسبات في بيتك خلال شبكه..
فمعنى ذلك انه يمكنك الاشتراكَ في الملفات، طابعات، نواسخ ضوئية(Scanner) ، والمشاركة في الاتصال بالانترنت.

بالاضافه إلى انه يمكنك اللعب بالألعاب (متعددة المستخدمين) على شبكتك .

الجدار الناري

هجوم هكرز





هو نظام حماية يقوم بمنع التسلل إلى داخل جهازك من أي جهاز آخر اكان ضمن شبكة داخلية أو شبكة خارجية.

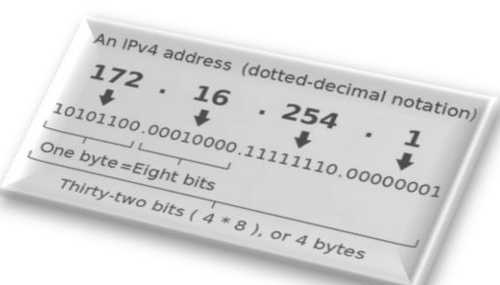
ينصح بشدة كل من يستخدم الكمبيوتر للانترنت أو في مجال شبكة داخلية أن يستخدم جدار ناري حتى لو كانت استخداماتك بسيطة.

وهو بطبيعة الحال يبطئ عمل الجهاز وهذا طبيعي جداً لأنه برنامج نشط ويراقب منافذ الجهاز ليتصيد أي عملية اختراق أو تسلل غير شرعي

ولكي تعمل مدى أهمية هذا النظام فجميع البنوك والشركات تستخدم أجهزة قوية وعملاقة للعمل كجدار ناري وهو الأساس في عملية السيكيورتي في الشبكة .

ما هو الاي بي ip address





الآي بي هو رقم يعطى لكل شخص يعمل كونيكت لشبكة الانترنت

و هو يتغير في كل مرة تدخل للشبكة

مامعني كلمة ip؟

internet protocol

بروتوكول الإنترنت

هل أن جهاز الحاسوب ذكي



حتى أن بعض الناس يضربه كمثل له بالذكاء والسرعة وقلة الأخطاء

ولكن.. هل هو ذكي فعلاً.؟؟؟
سأجاوبكم على هذا السؤال..



جهاز الحاسوب هو عبارة عن قطع إلكترونية متصلة مع بعضها يمر فيها تيار كهربائي لا يزيد عن ١٢ فولت
وهذا الجهاز لا يعمل بدون وجود نظام تشغيل مثبت عليه..

تقوم أنظمة التشغيل بتحديد مستوى ذكاء الحاسوب ..وهذا ما يسمى الذكاء الاصطناعي

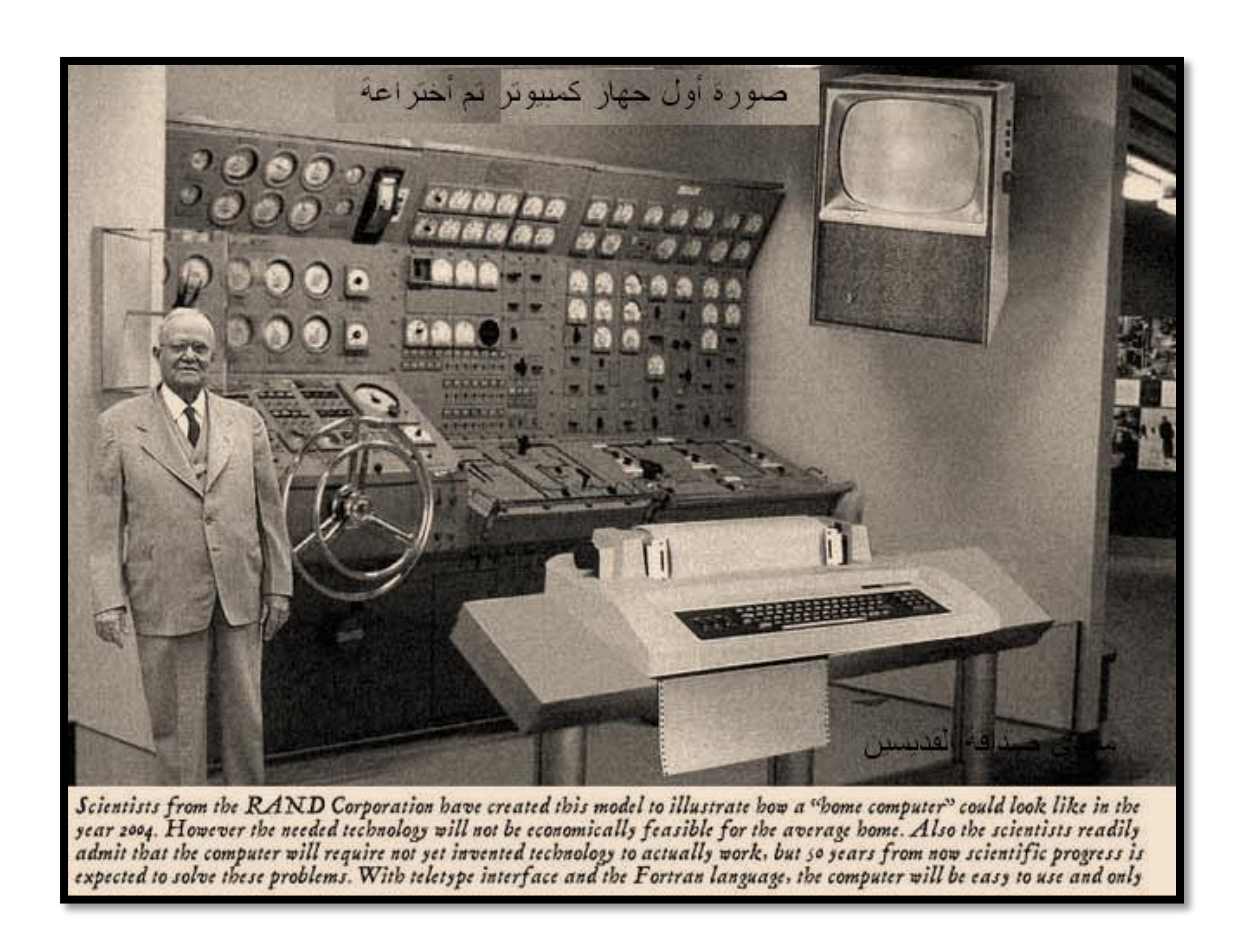
والسؤال التالي: من الذي قام ببرمجة وإنشاء أنظمة التشغيل؟؟؟؟



لا يمكن أن يكون شخص واحد.. لأنه لابد أن ينسى أو يسهو عن بعض الأمور ويخطئ في البعض الآخر..

ولكن هم عبارة عن مجموعة منتقاة من المبرمجين الذين يقومون بترتيب الأوامر والشروط التي يمر عليها الحاسوب وينفذها بنفس الترتيب المحدد ويقارنها.
وعمليات المقارنة هي التي تعطينا أغلب النتائج.

وفي هذه الحالة على المبرمجين أن يعملون على توقع جميع الاحتمالات لكي ينفذها ويقارنها الحاسوب.. وإلا فإنه سيظهر لنا رسائل لا معنى لها وربما توقف عن العمل.

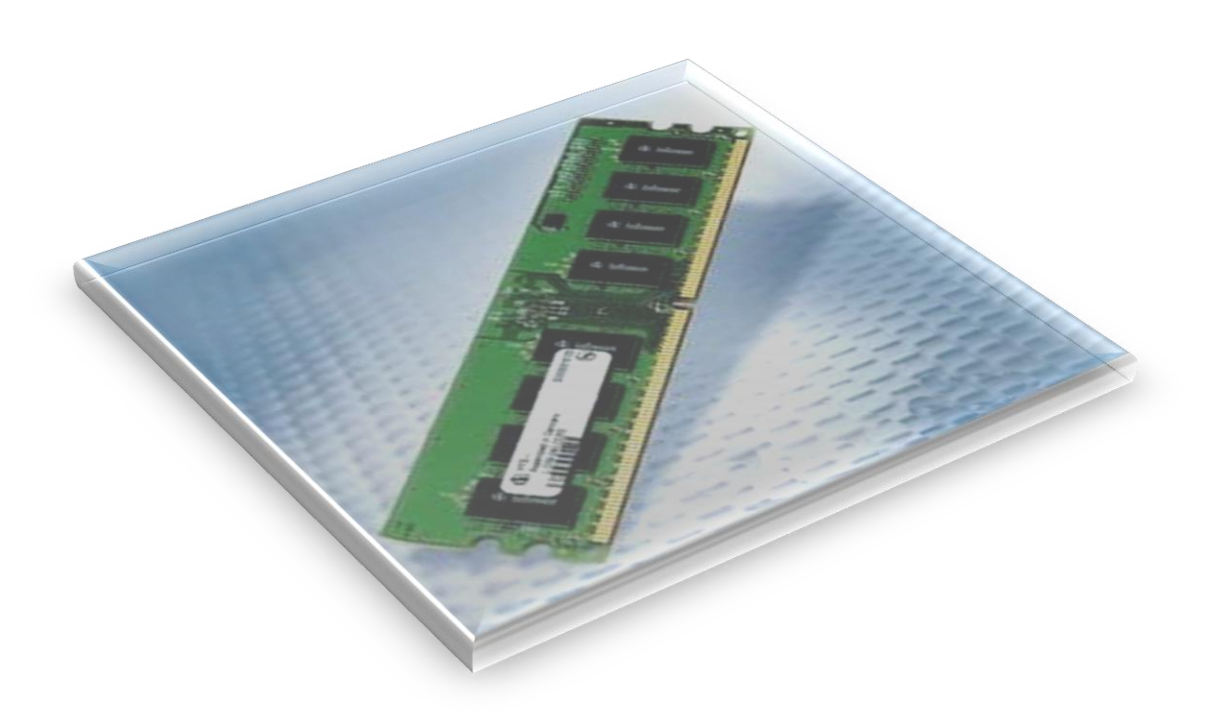


بعد ذلك تمر البرامج وأنظمة التشغيل بمرحلة التجربة والامتحان ..
وذلك بمساعدة العديد من المستخدمين ..
وهذا سبب نزول إصدار (Beta) في بعض البرامج ..أي أنه تجريبي..

بعد كل هذا، فإن سرعة تنفيذ الحاسوب لآلاف الأوامر تحدث في أجزاء من الثانية.
وهذا ما يحسسنا بالذكاء والسرعة.

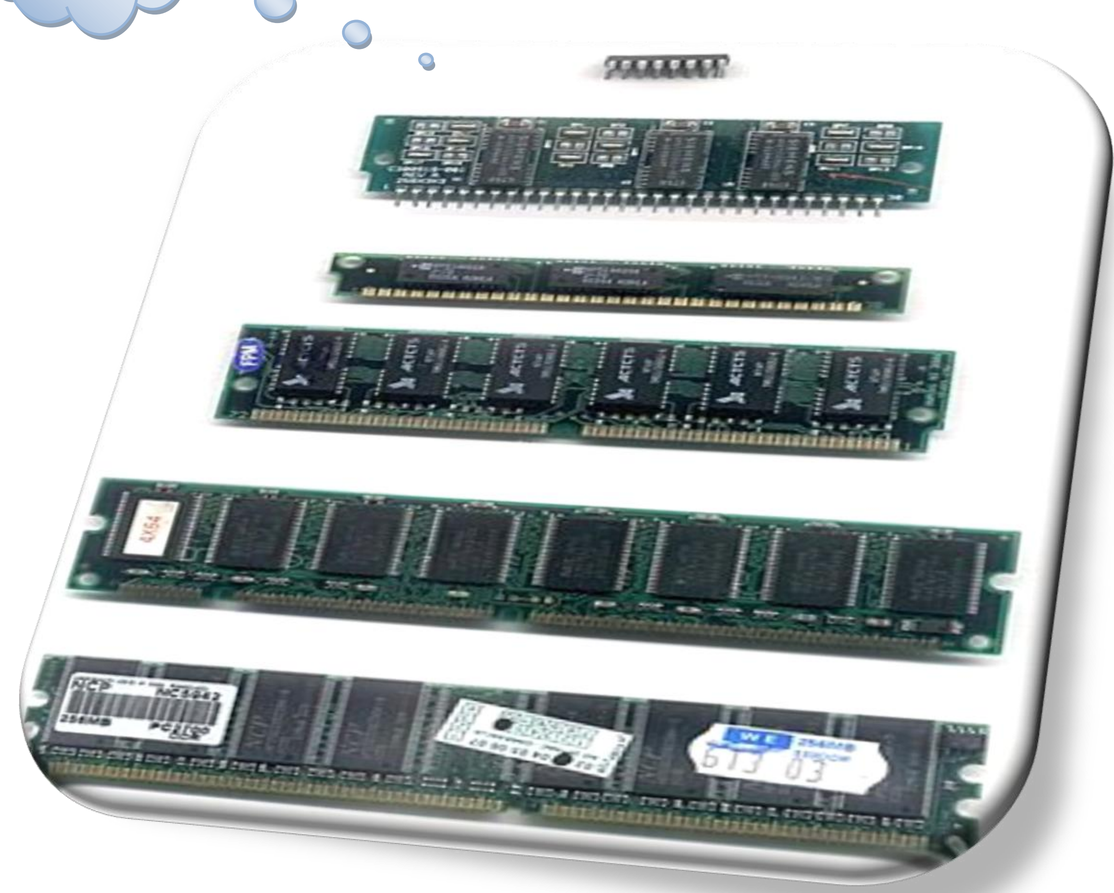
ومن هنا نكون قد تعلمنا ما هو سر ذكاء الحاسوب و ما هو تعريف الذكاء الاصطناعي.

الــــــرام:

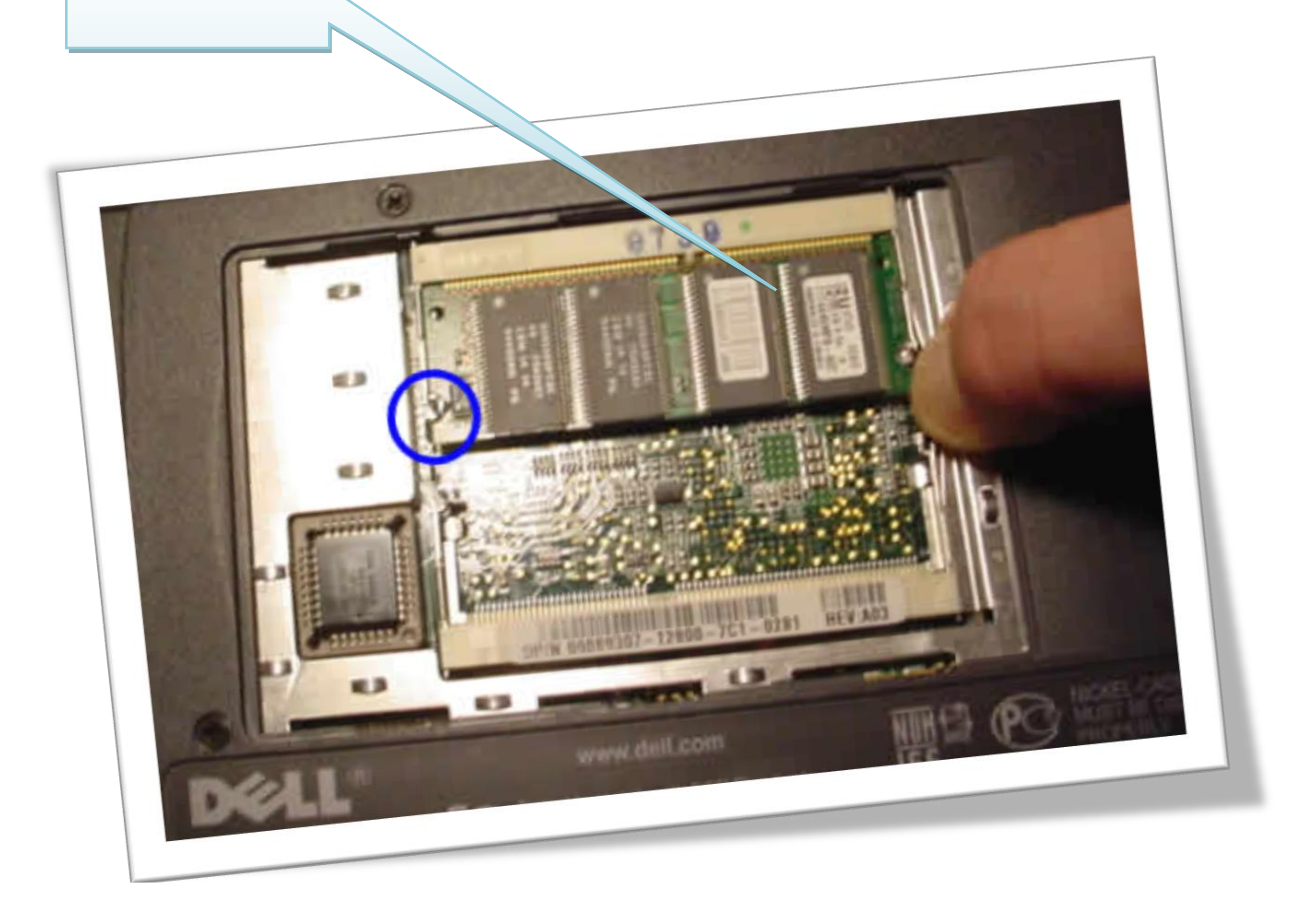


هو عبارة عن شريحة الكترونية تسمى بالذاكرة العشوائية وهي ذاكرة متقلبة يعني إذا تم إطفاء الجهاز كل المعلومات المحفوظة فيها تحذف..
سؤال شائع.. لماذا إذا فتح الجهاز لا يرفع الونيدز من القرص الصلب الى المعالج؟؟
هذا السؤال يوضح فائدة الرام..
عند تشغيلك للجهاز يقوم الرام بتحميل نظام التشغيل النظام الويندوز ليتم معالجة البيانات والمعلومات التي يقوم المستخدم بأجراءها على النظام كا تشغيل البرامج مثل برنامج الوورد عند



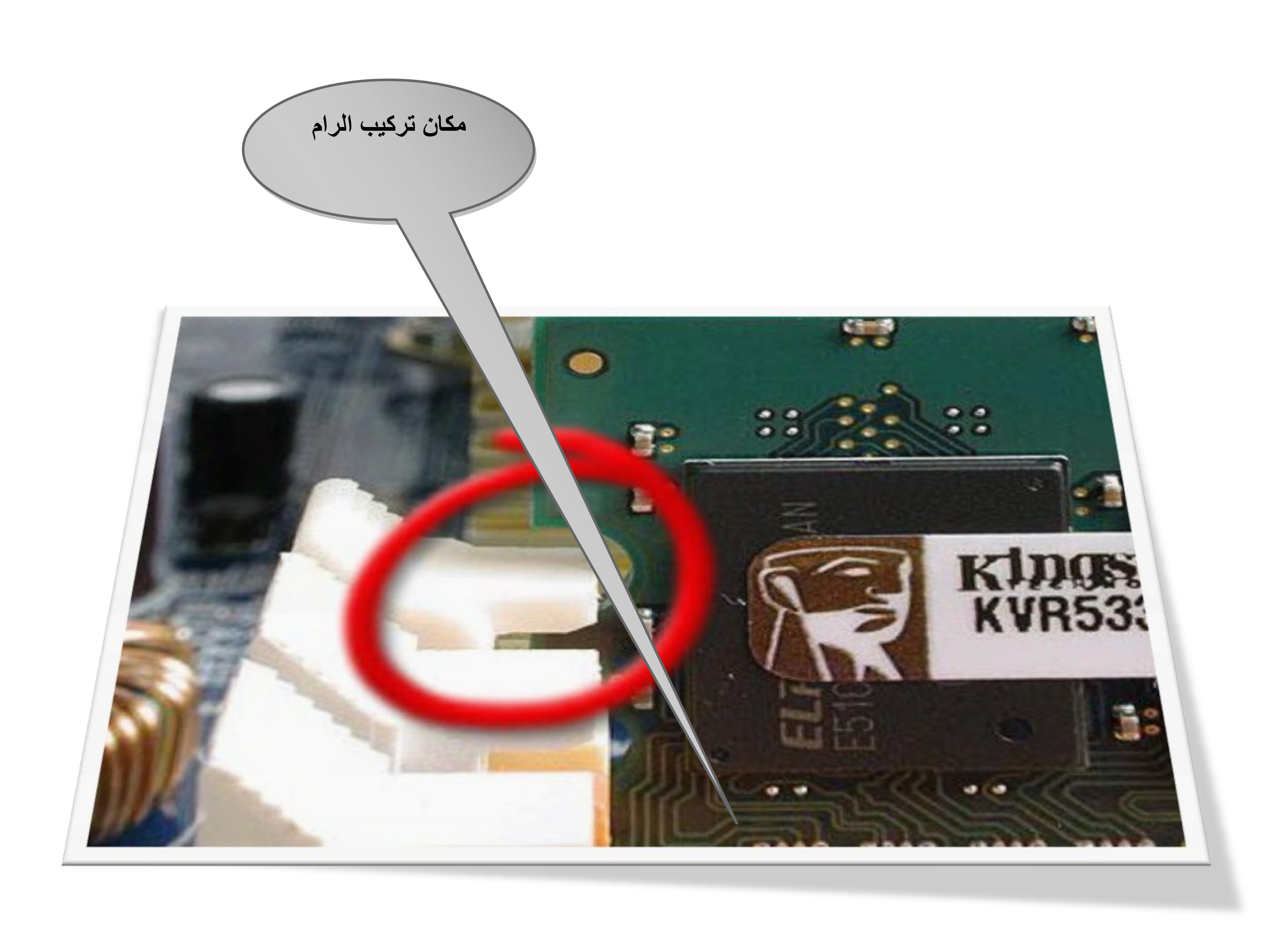


تشغيلك للبرنامج ماذا يحدث؟؟
يقوم المستخدم بطلب البرنامج بالنقر عليه نقر مزدوج يقوم الرام بطلب البرنامج من القرص الصلب وعندها يقوم المستخدم بكتابة نص ومعالجة هذا النص عن طريق المعالج وبعد الانتهاء من المعالجة حدث تغيير في البرنامج يقوم المستخدم بحفظ هذه التغييرات الملف

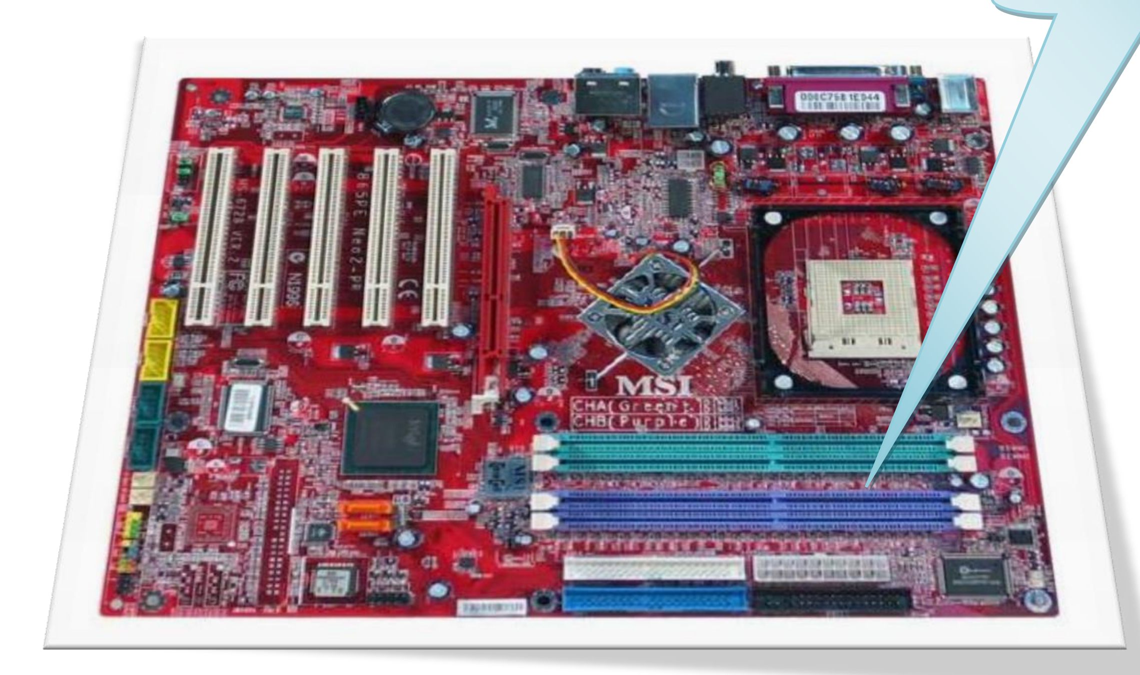


الصادر عن طريق أمر حفظ في برنامج الورود وبعدها المستخدم يغلق البرنامج.. هنا الرام تأخذ التغيير التي حفظت من قبل المستخدم او الملفات التي اصدرها هذا المستخدم.. وبعدها يقوم الرام بنقل هذا التغيير الى القرص الصلب لحفظه..

هنا الرام كالوسيط بين القرص الصلب والمعالج

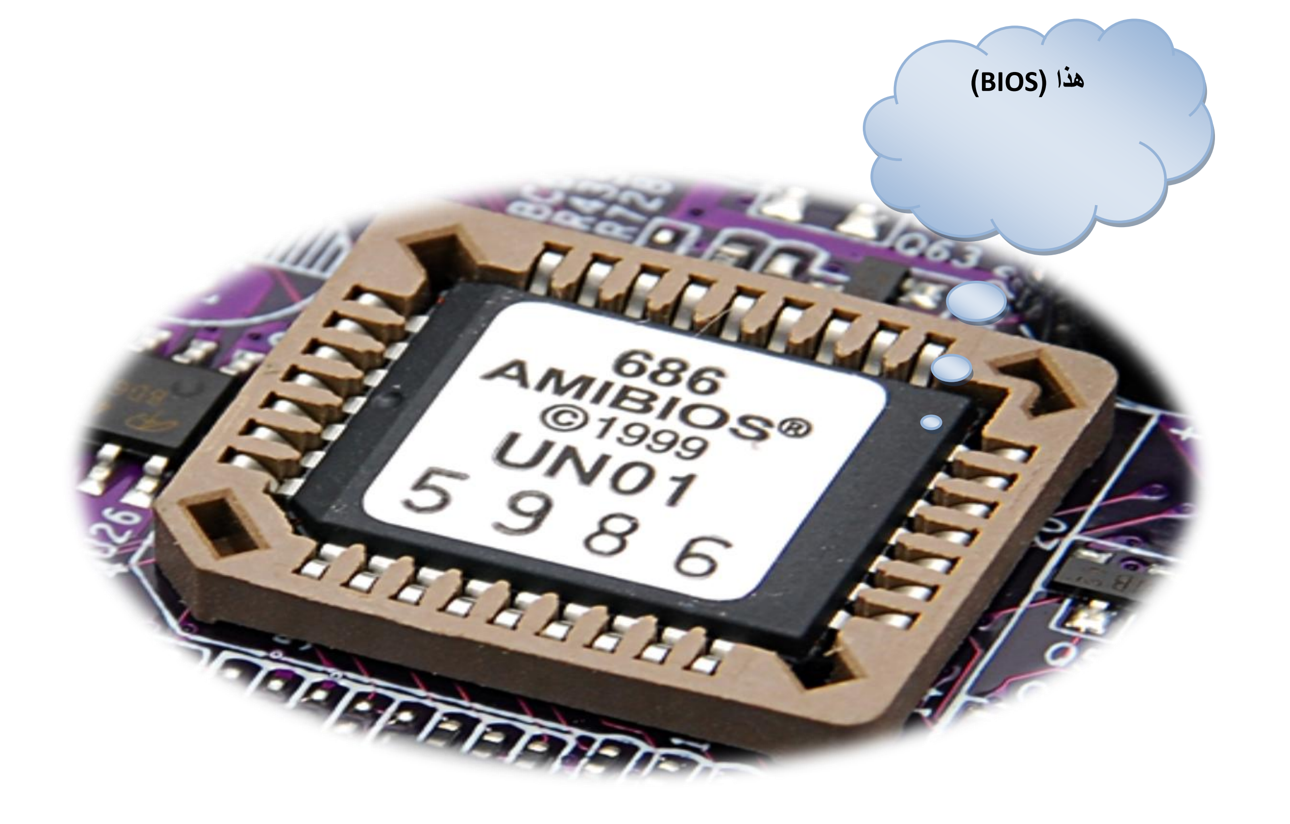


لان المعــالج ذو ســرعة عاليــه جــدا تصــل إلــى ١٦٦٦٦٦٦٦ نبضــة الكترونيــة فـي الثانيـة الوحدة تقريبا إذا قلنا إن سرعة الجهاز ٢٠٠٠ ميقاهرتز .. فــالرام ذو خاصــية الكترونيــة يســتطيع مجــارات سرعة المعالج بينما القرص الصلب ذو خاصية ميكانيكيــة لا يســتطيع مجــارات ســرعة المعــالج.. طبعا كلما زادت سعة الرام كلما زادت سرعة

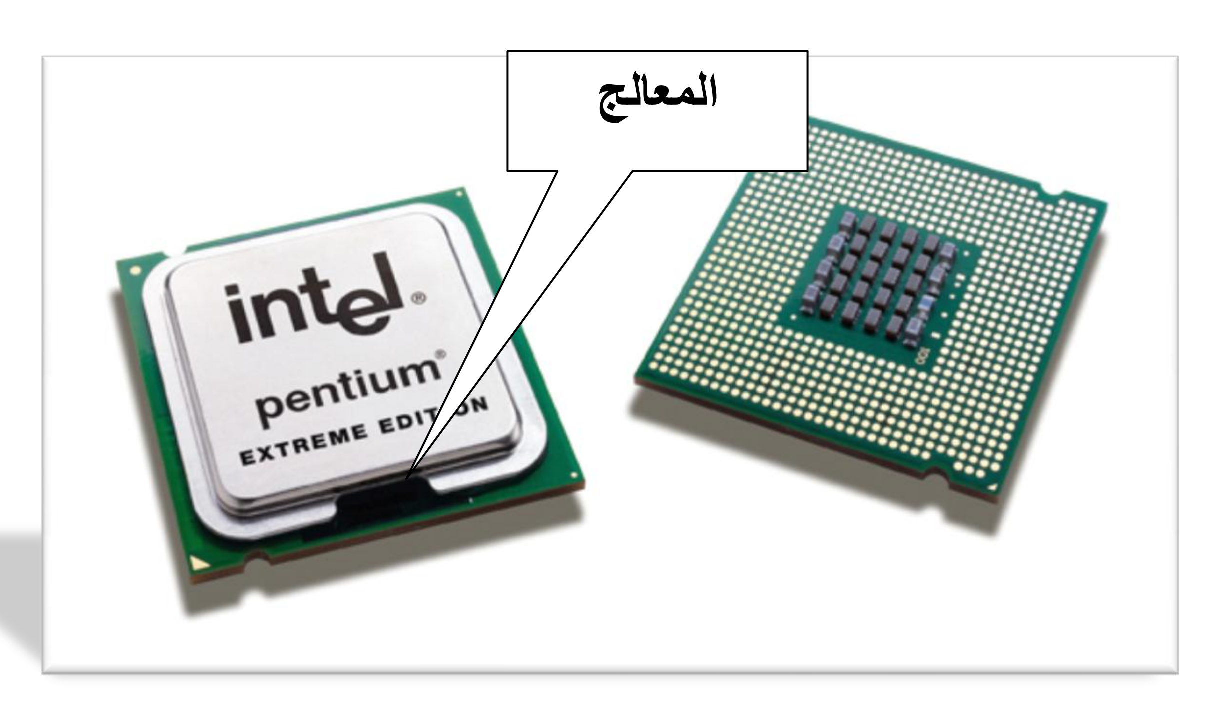


الجهاز..

ملاحظة : يقولون فيه برامج تسرع الويندوز
لا تسمع لهذه الاشياء لانها راح تضر جهازك.
الجهاز مثل جسم الانسان اذا انسان اخذ منشطات
عشان تزيد نشاطه فعلا المنشطات هذه تقوم بزيادة
نشاط جسم الإنسان لكن بالنهاية تضر الصحة



اذا كنت تريد سرعة جهازك تزيد   الرام .
أحيانا ..الكثير نزيد من حجم الرام   بشكل كبير
حتى تزيد من سرعة الجهاز ...لكن ..!! في نقطة
مهمة لازم ينتبه لها!!...
يجب يكون فيه توافق بين حجم الرام .. وسرعة
الناقل).. (BIOS) سرعة نقل البيانات من وإلى
الرام ...بمعنى   إن الرام كبير وسرعة الناقل تكون
بطيئة!!..



يكون فيه توافق بين حجم الرام وسرعة المعالج..
تخيل ... إن المعالج بطيئ جداً .. والرام فيه كمية بيانات كبيرة تنتظر
يكون فيه توافق بين حجم الرام ونوعية نظام

التشغيل المستخدم...
كمثال توضيحي ...



الوندوز ... XP يشترط عليك إن الرام عندك يكون ١٢٨ على الاقل ...

طيب اذا صار أقل!!..

في الحالة هذي .. الوندوز يكون بطيئ ... السبب إن الوندوز XP يستخدم ملفات كثيرة في الخلفية و مخفية تكون موجودة في الرام الذاكرة المؤقتة

الخلاصة:

إذا كنت تزيد الرام يجب الانتبها الى المواصفات جهازك .. مع العلم إنك لو زدته ومواصفات

جهازك ماتحتاج .... فإن الزيادة بتكون مهملة .. ومالها أي فايده...

توضح ألفكره أكثر ... تخيلو معي...



إن جهاز الكمبيوتر (مدرسة)

الهارديسك (مخزن المدرسة)

الرام (الفصل الدراسي)

الناقل (المستخدمين أو العامل)

البيانات (وسائل تعليمية مثلا)

مستخدمين الكمبيوتر(المدرس)

برنامج يحتاج بيانات (درس يحتاج وسيله تعليمة)

نظام التشغيل (مدير المدرسة)

فمثلا إذا الدرس يحتاج وسيلة تعليمية موجودة في المخزن ...فالمدرس يطلب من العامل أو المستخدم في المدرسة إنه يحضر له الوسيلة من المخزن إلى الفصل يشرح عليها مؤقتا ثم يرجعها)....طبعا كل العملية هذي ... المدير منظمها و لها قواعدها يديرها ...

بالضبط هذا الذي يصير داخل جهاز كل شخص البرنامج(الدرس) يشتغل في الرام (الفصل) .

وسيلة تعليمية



يحتاج إلى بيانات(وسيلة) ..نقوم بطلبها عن طريق الضغط أو الفتح للملفات(كأن المدرس ينادي المستخدم أو يرسل له طالب يناديه و هنا يقوم الناقل بنقل البيانات (عامل المدرسة يحضر الوسيله) من الهارديسك (المخزن) الى الرام

(الفصل) .. وكل العملية هذي تتم تحت عين نظام ***التشغيل (المدير)***

هل ألعاب الكمبيوتر تضيع وقت المعاق ذهنيا:



قد يعتقد البعض أن استخدام ألعاب الكمبيوتر مجرد تضيع لوقت الدارس (المعاق ذهنيا (أو تتويهه عن الواقع الذي يعشه .. فهذا فهم خطأ .. فكل خطوة يقوم بها المعاق ذهنيا على جهاز الكمبيوتر يتعلم شيء جديد .. ليس عن الكمبيوتر فحسب .. بل عن أشياء أخرى كثيرة هو في أشد الحاجة إليها .. وقد لا يستطيع أن يستوعبها (الدارس المعاق ذهنيا (بالطريقة التقليدية .. فهنا جاء دور الكمبيوتر.. للمساهمة في التعليم والترويح في ذات الوقت.

فوائد الكمبيوتر

في تأهيل ذوى الاحتياجات الخاصة

يوفر رد فعل ودعما فوريا

يوفر توجيهات وسبل المحاكاة

يساعد في عملية

التحفز

يساعد في عملية التركيز

يساعد في عملية التدريب والتطبيقات

يجنب الدارس من ذوى الاحتياجات الخاصة ..عند الخطأ ..الشعور بالحرج والفشل

يساعد على تنمية الاعتماد على الذات

التنويع في عرض الأشياء بصورة مشوقة للغاية

يعطى فرص كثيرة ومحاولات حتى ينجح الدارس في أداء المهمة المطلوبة

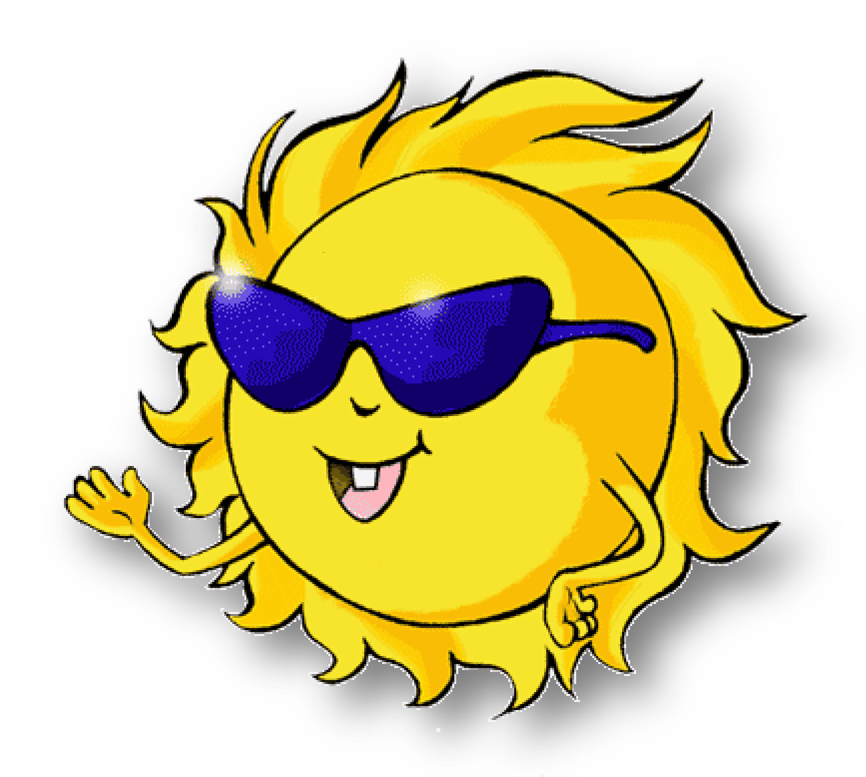
كل خطوة يقوم بها الدارس (المعاق) على الكمبيوتر يقابلها

استجابة من الكمبيوتر ثم يتم عرض درس أخر جديد مما يستلزم إجابة .. وبواسطة هذه الطريقة يحسن الدارس المعاق ذهنيا استخدام الوقت

-وسيلة من وسائل التعليم والترويح في ذات الوقت

-كسر الملل في عملية التدريس من خلال التنوع والإثارة

الحرارة الزائدة تسبب:



- تقصر من عمر المعالج
- تبطئ أدائه
- تتسبب بأخطاء في الحسابات

•تتسبب بتوقف الحاسب عن العمل بشكل متكرر (التعليق (

•قد يعيد الحاسب تشغيل نفسه بدون سبب

•قد تحدث أشياء غريبة مثل أخطاء في القرص الصلب

•في أحيان نادرة تؤدي لعطب المعالج كلياً .

أما سبب ارتفاع درجة حرارة المعالج أثناء العمل:

تعود إلى :

•كفاءة المبدد الحراري

•كفاءة مروحة التبريد

•كمية الحرارة التي ينتجها المعالج

•درجة حرارة علبة النظام ، حيث لا يمكن لأي مبدد حراري ومروحة أن يحفظ درجة حرارة المعالج إلى أقل من درجة حرارة علبة النظام ، هذا لأن الهواء الذي يدفع بين عواميد المبدد الحراري مأخوذ من علبة النظام نفسها .

•تصميم العلبة حيث أنه في علب النظام من نوع (Atx علب نظام بنتيوم الثاني وما بعده) تساعد العلبة نفسها في تبريد المعالج بتركيبها حيث يقع المعالج تحت مزود الطاقة ليكون في مجرى الهواء وهذا يساعد كثيراً في تفادي مشكلة الحرارة ، حتى أن هناك من يقول أن علب النظام Atx يمكن أن تبرد المعالج بالهواء الخارج من مزود

الطاقة .

إن أهم أسباب ارتفاع درجة الحرارة هو وجود الأوساخ على المبدد الحراري مما يعيق مرور الهواء فيه

لعبة الأطفال مع الكمبيوتر:



إذا كان في مكان عملك أكثر من حاسب شخصي ففي الغالب أنت
تستخدم شبكة لكي تتصل هذه الحاسبات ببعضها البعض وأيضا إذا
كان في منزلك أكثر من حاسب فسوف تجد من المفيد أن تصل هذه
الحاسبات معا وأن تجعلها تكلم بعضها .إيصال الحاسبات في شبكة
لها عدة طرق منها أن تتصل الحاسبات بكابل وتتجمع هذه الكابلات
في جهاز توزيع يطلق عليهHub

وهذه الطريقة هي أقدم الطرق لإنشاء شبكة حاسبات محلية LAN
وتستخدم منذ عشرات السنوات. قد لا تكون هذه الطريقة مناسبة إذا
لم تتوفر مسارات مناسبة للكابلات أو إذا لم يكن مناسبا تكسير
الحوائط لمد كابلات الشبكة. إذا كان لديك خط إنترنت سريع
بالمنزل أو بمكان العمل من نوع ADSL فسوف يكون من
الأفضل أن تستخدم تقنية Wi-Fi لكي تتمكن من الاتصال بشبكة
الإنترنت لاسلكيا. الاتصال اللاسلكي يعتبر أحد طرق توصيل
الحاسبات ببعضها البعض لكي تكون شبكة وفي حالة اتصالك
بالإنترنت سواء سلكيا أو لاسلكيا فأن حاسبك يعتبر جزء من هذه
الشبكة العالمية. من مزايا الشبكات اللاسلكية أنك تستطيع أن تضع
حاسبك في أي مكان فأنت غير مقيد بالمكان الذي يوجد به الكابل
كما أنك تستطيع أن تغير مكان الحاسب كما تريد طالما أنت في
المدي الذي تصل إليه الشبكة اللاسلكية. في شبكات الحاسبات
اللاسلكية من نوع Wi-Fi تتصل الحاسبات ببعضها البعض عن
طريق موجات الراديو Radio Signals طالما كانت هذه
الحاسبات لا تبعد عن الجهاز الذي يبث هذه الموجات بمسافة 100
قدم أي حوالي ٣٠ متر.

أجهزة الوكي توكي:

أبسط مثال لكي نتعرف علي طريقة عمل الشبكات اللاسلكية-Wi-Fi هو أن نتذكر لعبة الأطفال التي تباع في محال اللعب ويطلق عليها وكي توكي وتتكون من علبتين بلاستيك صغيرتين يوضع بكل منها جهاز صغير يستطيع إرسال واستقبال موجات الراديو. عندما يتكلم الطفل في الجهاز يتم نقل الصوت عبر ميكروفون ويتم تحويله إلي موجات راديو ثم ينطلق عبر الهوائي (اريال) الذي يوجد في هذه اللعبة. الطرف الثاني والذي يوجد ربما في غرفة أخري يستقبل إرسال الراديو عن طريق الهوائي ثم يقوم الجهاز بتحويل موجات الراديو إلي صوت يتم نقله إلي سماعة الجهاز. قوة موجات هذه اللعبة تبلغ حوالي ربع وات وتستطيع نقل الصوت لمسافة قد تصل إلي ١٠٠ متر تقريبا. إذا تخيلنا أننا نريد أن نصل حاسبين بنفس الطريقة التي تعمل بها هذه اللعبة فنحن نحتاج إلي:

***يحتاج كل حاسب إلي وحدة تحول البيانات الرقمية التي توجد به إلي موجات راديو والعكس.

***يحتاج كل حاسب إلي وحدة إرسال واستقبال لموجات الراديو

الشبكات اللاسلكية التي تستخدم تقنية WiFi تعتبر الأكثر إنتشار في العالم الآن. أجهزة لعب الأطفال اللاسلكية التي يطلق عليها وكي توكي تستخدم موجات الراديو التي تستخدم في شبكات الحاسبات اللاسلكية. هذه اللعبة لديها القدرة علي ارسال واستقبال موجات الراديو ولكن هناك ثلاث فروق رئيسية بين لعبة الوكي توكي وتقنية WiFi التي تستخدم في الشبكات اللاسلكية:

***الشبكات اللاسلكية التي تستخدم تقنية WiFi من نوع

٨٠٢.١١ b و802.11g تستطيع أن ترسل موجات الراديو بتردد يصل الي ٢.٤ جيجاهرتز ونوع ٨٠٢.١١ aترسل الموجات بتردد ٥ جيجاهرتز أما لعبة الوكي توكي فتستخدم تردد ضعيف لا يزيد عن ٥٠ ميجاهرتز (الجيجاهرتز حوالي ١٠٠٠ ميجاهرتز) وكلما زاد التردد المستخدم كلما أمكن أرسال واستقبال البيانات بسرعة أعلي.

***تستخدم تقنية WiFi تقنية لبث البيانات عبر موجات الراديو أكثر كفاءة من من تلك التي تستخدم في ألعاب الوكي توكي.

***التقنية التي تستخدمها WiFi لديها القدرة علي تغير التردد فمثلا تقنية ٨٠٢.١١ bتستطيع التعامل مع ثلاث سرعات من الترددات. كما يمكنها أن تقسم التردد المستخدم الي عشرات القنوات channelsوبذلك تمكن عشرات الحاسبات من التعامل بتردد واحد دون أن تتداخل البيانات بينهم.

نظرا لقدرة تقنية WiFi علي التعامل بتردد أقوي وبكفاءة أعلي فإنها تسطيع ارسال واستقبال البيانات بسرعة أعلي .كروت الاتصال التي تستخدم تقنية ٨٠٢.١١ bتستطيع أن ترسل البيانات بسرعة تصل الي ١١ ميجابيت في الثانية بينما تقنية ٨٠٢.١١ a وتقنية ٨٠٢.١١ gتستطيع ارسال البيانات بسرعة ٥٤ ميجابيت في الثانية.

الاسماء الغريبة لتقنية WiFi مثل ٨٠٢.١١ aترجع الي الاسم الذي اختاره المعهد الهندسي للمواصفات القياسية الكهربائية والإلكترونية الأمريكي والذي يطلق عليه IEEE حيث اختار الأرقام ٨٠٢.١١ لكي يعبر عن المواصفات القياسية لتقنية

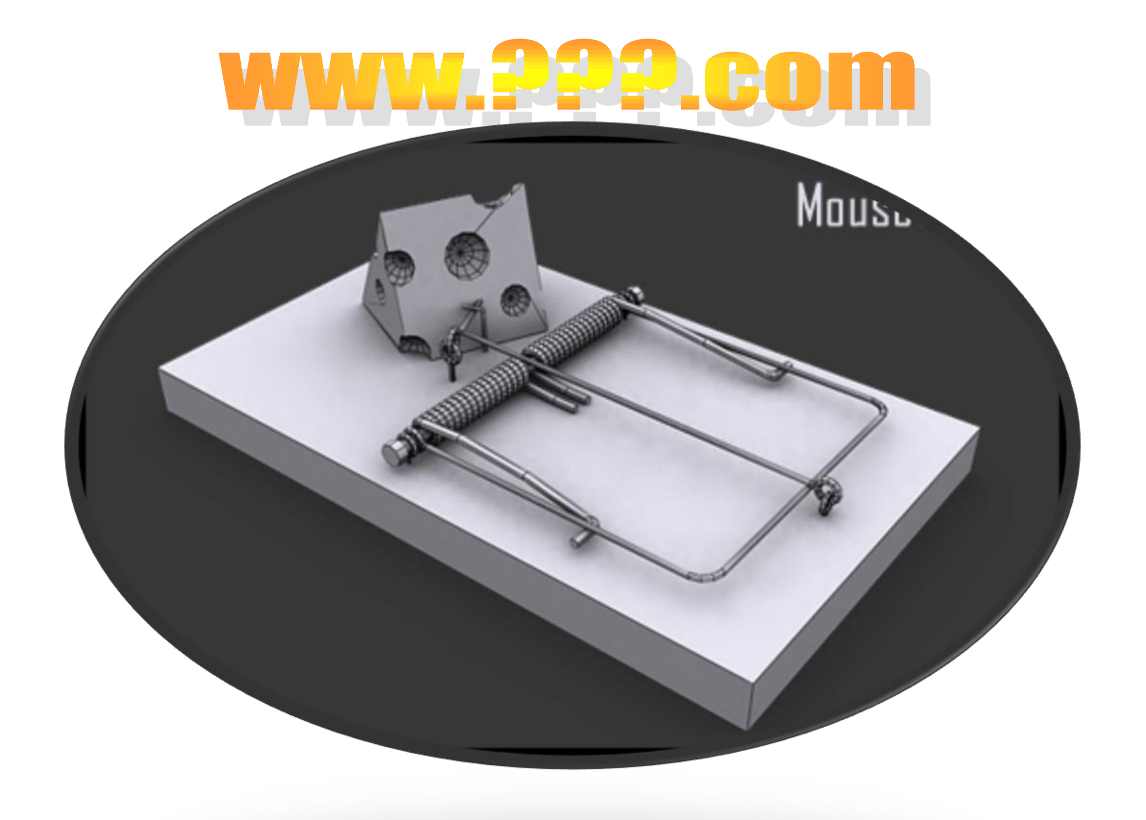
الاتصالات اللاسلكية WiFi أما الحرف التالي لهذا الرقم فهو يعبر عن التطور الذي حدث لهذه التقنية:

***الحرف b يعبر عن النسخة الأولي من تقنية WiFi التي وصلت الي أسواق الحاسبات العالمية وهي الأكثر بطأ والأقل سعرا. هذه النسخة من التقنية تستطيع نقل البيانات بسرعة ١١ ميجابت في الثانية.

***الحرف a يرمز للنسخة التالية الأكثر تطورا حيث تستخدم تردد يصل الي ٥ جيجاهرتز وتستطيع نقل البيانات بسرعة ٥٤ ميجابت في الثاني.

***أما الحرف g فيرمز الي تقنية خليطة بين النوعين السابقين فهي تستخدم تردد أقل من النوع السابق وهو ٢.٤ جيجارهتز ولكنه ينقل البيانات بنفس السرعة العالية وهي ٥٤ ميجابت في الثانية.

نقرأ كثيرا في إعلانات الحاسبات المحمولة الحديثة عن التقنية التي يستخدمها في الاتصال اللاسلكي بالشبكات ومن المعلومات السابقة سوف نتمكن من تفسير المصطلحات التي توجد في هذه الإعلانات



المحتالون موجودون منذ الأزل، والآن في عصر الإنترنت هم ينتشرون على ويب، فيبحثون عن فريسة من المستهلكين غير الحذرين عبر إنترنت. ويتصاعد معدل الاحتيال عبر إنترنت، وتتطور أساليب إنشاء رسائل البريد الإلكتروني ومواقع ويب الاحتيالية. تعرف على المزيد حول كيفية حماية نفسك من الاحتيال عبر إنترنت.

ما هو الخداع أو التصيد الاحتيالي عبر إنترنت؟

التصيد الاحتيالي هو أسلوب احتيال عبر إنترنت يستخدمه المجرمون لإغرائك بالقيام بالكشف عن معلوماتك الشخصية. يعتبر التصيد الاحتيالي أسرع وسائل ارتكاب الجرائم عبر إنترنت وأكثرها انتشارًا وتستخدم لسرقة الأموال الشخصية واختراق الهويات وسرقتها .

يستخدم المحتالون العديد من الأساليب المختلفة لخداعك، بما في ذلك البريد الإلكتروني ومواقع ويب التي تحاكي العلامات التجارية المعروفة والموثوقة. من الممارسات الاحتيالية الشائعة إرسال "البريد الإلكتروني العشوائي" الذي يتضمن رسائل زائفة تشبه الرسائل السليمة والصحيحة من موقع ويب معروف أو شركة يثق المستلمون بها، مثل شركات بطاقات الائتمان أو البنوك أو الجمعيات الخيرية أو مواقع التسوق للتجارية عبر إنترنت. والغرض من هذه الرسائل الزائفة هو خداع المستهلكين كي يقوموا بتوفير المعلومات الشخصية التالية:

- الاسم واسم المستخدم .

- العنوان ورقم الهاتف .
- كلمة المرور أو رقم التعريف الشخصي (PIN).
- رقم حساب البنك .
- رقم بطاقة الائتمان أو الإيداع/الصراف الآلي .
- رمز التحقق من صحة بطاقة الائتمان (CVC)أو قيمة إثبات البطاقة .(CVV)
- رقم الضمان الاجتماعي (SSN)

يستخدم المجرمون هذه المعلومات بطرق عديدة للكسب المالي. على سبيل المثال، تعتبر سرقة الهويات الشخصية إحدى الممارسات العامة حيث يقوم المجرم بسرقة معلوماتك الشخصية وانتحال هويتك، ويمكنه بعد ذلك القيام بما يلي:

- طلب ائتمان والحصول عليه باسمك .
- إفراغ الحساب البنكي الخاص بك واستنفاد كامل المبلغ المسموح به في بطاقات الائتمان .
- نقل الأموال من حسابات استثمارية أو خط ائتمان إلى حساب جارٍ، ثم استخدام نسخة

من بطاقة الإيداع للسحب نقداً من الحساب الجاري باستخدام أجهزة الصراف الآلي (ATM)في أي مكان في العالم .

أمثلة لمخططات التصيد

تشمل بعض الأمثلة عن مخططات التصيد:

- رسائل البريد الإلكتروني الزائفة التي تبدو وكأنها من شركة تعمل معها، والتي تعلمك بأن الشركة تحتاج إلى التحقق من معلومات الحساب الخاص بك أو أنه قد يتم إيقاف هذا الحساب .
- مجموعة من مواقع المزاد الاحتيالية ومواقع الرهان الزائفة. يحدث هذا عند عرض مواد للبيع في مزاد شرعي عبر إنترنت لإغرائك بدفع مبالغ مالية إلى موقع رهان زائف .
- عمليات البيع الزائفة عبر إنترنت، حيث يعرض عليك أحد المجرمين شراء شيء ما منك، ويطلب أن يدفع لك مبلغًا أعلى بكثير من السعر المحدد للسلعة التي يشتريها. وفي المقابل، يطلب منك إرسال شيك بفارق المبلغ. وبعدها لا يتم الدفع لك، في حين أنه

يتم صرف الشيك الخاص بك، ويحصل المجرم على الفارق. إضافةً إلى ذلك، يضم الشيك الذي ترسله رقم الحساب البنكي الخاص بك ورمز المسار البنكي والعنوان ورقم الهاتف .

- الجمعيات الخيرية الزائفة التي تطلب منك نقودًا. للأسف، يستغل العديد من المجرمين نيتك الحسنة .

هناك المزيد من مخططات التصيد المستخدمة. للحصول على تقرير محدَّث بشأن مخططات

كيف يمكنني أن أعرف إذا كانت رسالة البريد الإلكتروني احتيالية أم لا؟

للأسف، مع تطور أساليب عمليات التصيد الاحتيالي، يصعب جدًا على الإنسان العادي معرفة ما إذا كانت الرسالة احتيالية أم لا. ذلك هو السبب في الانتشار الواسع لمخططات التصيد ونجاح المجرمين بتنفيذها. على سبيل المثال، فإن العديد من رسائل البريد الإلكتروني الزائفة ترتبط بشعارات لشركات حقيقية ذات علامات تجارية

معروفة .ولكن هناك بعض الأشياء التي يمكنك البحث عنها والتحقق منها:

- **طلب معلومات شخصية في رسالة البريد إلكتروني** تتخذ معظم الشركات الشرعية نهجاً وهو ألا تطلب منك معلومات شخصية عبر البريد الإلكتروني. لا تثق في أية رسالة تطلب منك معلومات شخصية حتى وإن بدت شرعية .
- **الصيغة واللهجة الملحة** تكون اللغة المستخدمة في رسائل التصيد الإلكترونية عادةً ذات لهجة مهذبة ولطيفة. إنها غالباً ما تحاول جذبك للاستجابة إلى الرسائل أو للنقر فوق الارتباط الذي تتضمنه الرسالة. ولزيادة عدد الاستجابات، يحاول المجرمون خلق طابع من الإلحاح يستجيب له المتلقون في الحال دون تفكير. وعادةً، تكون رسائل البريد الإلكتروني الاحتيالية غير شخصية وغير مخصصة، في حين أن الرسائل الصحيحة والسليمة التي ترد من البنك أو شركة تجارة إلكترونية تكون عامةً

مخصصة وشخصية. في ما يلي مثال عن مخطط تصيد فعلي:

أيها العميل المصرفي العزيز، أُحطنا علماً بضرورة تحديث معلومات الحساب لدينا نظراً لوجود عضو غير نشط وعمليات احتيال وتقارير انتحال. سيؤدي عدم تحديث السجلات إلى إلغاء الحساب. الرجاء اتباع الارتباط أدناه للتأكيد على بياناتك .

- **الارتباطات الزائفة** أصبح المحتالون أكثر تطورًا في قدرتهم على إنشاء ارتباطات خادعة لدرجة أنه يستحيل على الشخص العادي معرفة ما إذا كان الارتباط شرعيًا أم لا. يُستحسن دائمًا كتابة عنوان ويب أو عنوان محدد موقع المعلومات URL الصحيح في المستعرض. كذلك، يمكن حفظ محدد موقع المعلومات (URL) الصحيح في "مفضلة" المستعرض .*لا تقم بنسخ عناوين URLولصقها من الرسائل إلى المستعرض الخاص بك* .من الأساليب التي استخدمها

المجرمون في الماضي لتزييف الارتباطات ما يلي :

- في الرسائل التي هي بتنسيقHTML ، قد يحتوي الارتباط الذي يتم حثك على النقر فوقه على اسم شركة حقيقية، ويكون الاسم كاملاً أو جزءاً منه، وقد يكون الاسم مقنعًا، ما يعني أن الارتباط الذي تراه لا ينقلك إلى العنوان المطلوب، بل إلى موقع آخر مختلف، غالبًا ما يكون موقع ويب مزيف. لاحظ في هذا المثال أن وضع المؤشر على الارتباط في رسالة Outlook يكشف عن عنوان إنترنت رقمي آخر في المربع ذي الخلفية الصفراء. ينبغي أن يثير هذا في نفسك الشكوك .

https://www.woodgrovebank.com/loginscript/user2.jsp
http://192.168.255.205/wood/index.htm

- احذر من محددات مواقع المعلومات (URL)التي تتضمن العلامة @. في المثال التالي، ينقلك عنوان URL إلى الموقع الذي يأتي بعد علامة @ وليس

إلى بنك Wood Grove. ذلك لأن المستعرضات تتجاهل أي عنصر يسبق العلامة @ في محدد موقع المعلومات URL:

https://www.woodgrovebank.com@nl.tv/secure_verification.aspx

من المحتمل جداً أن يكون الموقع الحقيقي **nl.tv/secure_verification.aspx** موقعاً غير آمن.

- ومن الأساليب الشائعة الأخرى التي تم استخدامها، عنوان URL يبدو لأول وهلة كاسم لشركة معروفة ولكن يتضح أنه محرف قليلاً عند التدقيق فيه. على سبيل المثال، قد يظهر بدلاً من www.microsoft.com:

www.micosoft.com

www.verify-microsoft.com

www.mircosoft.com

لقد كسبت Microsoft مؤخرًا العديد من الدعاوى القضائية ضد أفراد استخدموا هذه الأنماط من عناوين URLللاحتيال على ممتلكات Microsoftالشرعية. ولكن هذه الممارسات تظل مستخدمة ومنتشرة وغالبًا ما تتم حمايتها بواسطة الحدود القومية.

نص الرسالة عبارة عن صورة لتجنب الكشف بواسطة عوامل تصفية رسائل البريد العشوائي، غالبًا ما تستخدم رسائل البريد الإلكتروني المزيفة في مخططات الاحتيال صورة بدلاً من النص في موقع النص الرئيسي للرسالة. إذا ما استخدمت رسالة البريد العشوائي المرسلة نصًا حقيقيًا، فإن تصفية البريد الإلكتروني غير الهام لـ Outlookستقوم بنقل الرسالة إلى مجلد **البريد الإلكتروني غير الهام** .وعادةً، تكون صورة النص الرئيسي للرسالة عبارة عن ارتباط .يمكنك التعرف عليه لأنه عند

تحريك مؤشر الماوس فوق النص الرئيسي للرسالة، يتحول المؤشر إلى شكل يد.

عفوًا، إننا نطالبك بإتباع المرجع المتوفر
أدناه لتأكيد بياناتك، وإلا فإنه
سيتم منع وصولك إلى النظام.

يمكن ربط أنواع أخرى من الصور التي يتم وضعها في رسائل البريد الإلكتروني بخادم المحتال، وتلعب دور إشارات ويب .عندما تقوم بفتح رسالة بريد إلكتروني، يتم تنزيل الصور ويتم إرجاع معلومات إلى الخادم. يتم استخدام هذه المعلومات للتحقق من أن عنوان البريد الإلكتروني الخاص بك صالح ولذلك قد يتم إرسال رسائل بريد إلكتروني غير هامة إليك مرة أخرى. يقوم Outlook افتراضيًا وبشكل تلقائي بحظر هذه الأنواع من الصور الخارجية. لمزيد من المعلومات، انظر حول حماية الخصوصية بواسطة حظر تنزيلات الصور التلقائية.

المرفقات تطلب منك الكثير من مخططات التصيد فتح مرفقات قد تصيب جهاز الكمبيوتر الخاص بك بـفيروس أو برامج

تجسس .إذا تم تنزيل برنامج تجسس إلى جهاز الكمبيوتر الخاص بك، فبإمكانه تسجيل ضغطات لوحة المفاتيح التي تستخدمها للدخول إلى حساباتك الشخصية عبر إنترنت ثم يقوم بإرسال هذه المعلومات إلى المجرم. لذلك، تأكد من عدم فتح أية مرفقات توجد في رسائل بريد مشكوك فيها. يجب أولاً حفظ أية مرفقات تريد رؤيتها، ثم تفحصها باستخدام برنامج مكافح للفيروسات محدَّث قبل فتح هذا المرفق. للمساعدة في حماية جهاز الكمبيوتر الخاص بك، يقوم Outlookو Microsoft Outlook Expressتلقائيًا بحظر أنواع ملفات مرفقة معينة بإمكانها نشر فيروسات. لمزيد من المعلومات، انظر كيف يساعد Outlook على حماية الكمبيوتر من الفيروسات .

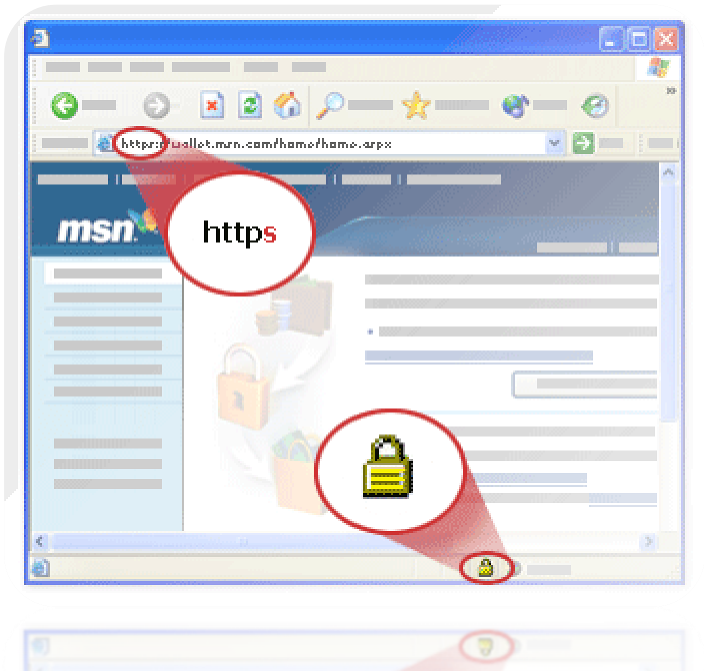
الوعود المبالغ فيها توخ الحذر من أية رسائل يتم عرض أموال أو خصومات فيها بشكل مبالغ فيه .

كيف يمكنني معرفة ما إذا موقع ويب معين هو موقع احتيالي أم لا؟

مقارنة برسائل البريد الإلكتروني الاحتيالية، فإن مواقع ويب المزيفة تحتوي على رسومات شعارات وارتباطات ويب مقنعة، مما يجعل من الصعب معرفة ما إذا كانت هذه المواقع احتيالية أم لا. أفضل وسيلة هي عدم النقر فوق الارتباطات الموجودة في الرسائل المشكوك فيها. من الأشياء التي يتعين عليك البحث عنها والتي تتوفر في مواقع ويب الشرعية ما يلي :

- **أمان SSL** تستخدم مواقع ويب الشرعية طبقة مآخذ التوصيل الآمنة (SSL) أو أي تقنية أمان أخرى تساعد على حماية المعلومات الشخصية التي تدخلها عند فتح حساب جديد وعند تسجيل الدخول إلى الموقع بعد ذلك. تتم الإشارة إلى حالة الأمان في شريط معلومات المستعرض الخاص بك بواسطة رمز قفل. إضافةً إلى أن عنوان ويب يُسبق بـ) **https://** لاحظ أن **s** الموجودة بعد **http** تشير إلى **الأمان** (بدلاً من البادئة المعتادة **http://** في شريط

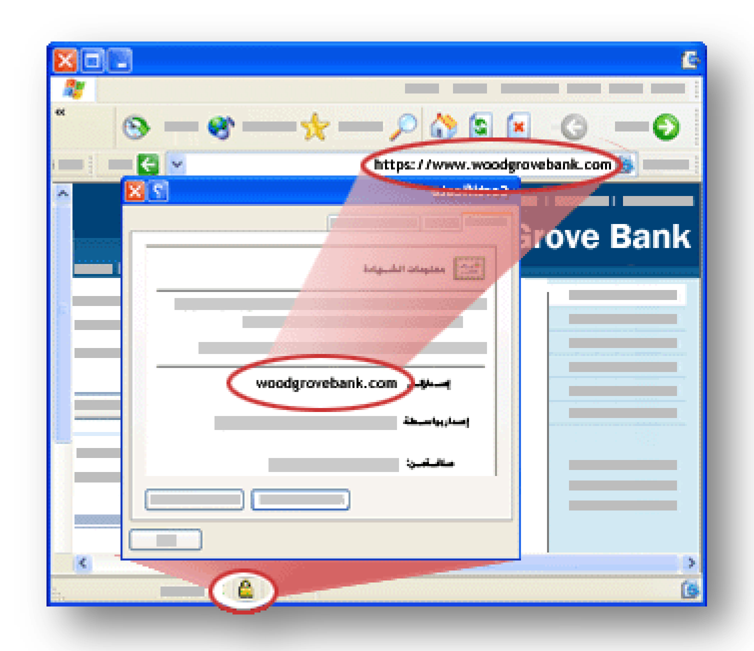
عنوان المستعرض.



هام لاحظ أنه، أحياناً قد يتم تزييف **https://**في الارتباطات، كما هو الحال في مثال "الارتباط المقنع" المعروض في القسم "ارتباطات مزيفة."

- **شهادة رقمية لموقع ويب** الفائدة الإضافية لـ SSL هي المصادقة – عملية التعرف على موقع ويب لك. توفر SSL هذه الفائدة من خلال استخدام شهادة رقمية، والتي يقدمها الموقع للمستعرض الخاص بك عند اتصالك. لعرض الشهادة، انقر نقرًا مزدوجًا

فوق رمز القفل الموجود في الزاوية السفلية اليسرى من المستعرض وتحقق من حقل **صادر لأجل**. يجب أن يتطابق الاسم الموجود على الشهادة مع الموقع الذي تعتقد أنك فيه. على سبيل المثال، إذا كانٍ الموقع فعلاً هو بنكWood Grove ، إذًا فإن اسم حقل **صادر لأجل** يجب أن يطابق عنوان URL **woodgrovebank.com**. إذا كان الاسم مختلفًا، فقد تكون في موقع مزيف. ومرة أخرى أدعوك إلى توخي الحذر ومراعاة الأخطاء الإملائية الصغيرة. إذا انتهت صلاحية الشهادة، أو لم يتم التوثيق عليها بواسطة مرجع مصدق أو أنها تحتوي على اسم لا يتطابق مع الاسم المعروض في شريط العنوان، يعرض Microsoft Internet Explorerرسالة تحذير .



لمعرفة المزيد عن الشهادة، انقر فوق علامة التبويب **تفاصيل**. إذا لم تكن متأكدًا مما إذا كانت الشهادة شرعية أم لا، فلا تدخل أية بيانات شخصية. أمِّن نفسك، وغادر موقع الويب. للتعرف على المزيد من الطرق التي يمكن من خلالها تحديد ما إذا كان الموقع آمنًا أم لا، قم بقراءة كيف يساعد Internet Explorerعلى الاحتفاظ بالبيانات آمنة.

أفضل الممارسات للمساعدة في الحماية من الاحتيال عبر إنترنت

عدم الرد على أي رسالة بريد إلكتروني تطلب معلومات شخصية لا تثق بأي رسالة

إلكترونية ترد من عمل أو شخص يطلب منك معلومات شخصية خاصة بك ـــ أو يرسل لك معلومات شخصية ويطلب منك تحديثها أو تأكيدها. بدلاً من ذلك، استخدم رقم الهاتف من أحد البيانات الخاصة بك للاتصال. لا تطلب أي رقم ورد في رسالة البريد الإلكتروني. وبالمثل، لا تقدم أي معلومات خاصة طواعيةً لشخص ما يجري اتصالاً بك غير مرغوب فيه .

عدم النقر فوق أي ارتباط موجود في رسالة بريد إلكتروني مريبة لا تقم بالنقر فوق أي ارتباط موجود في رسالة مريبة. قد يكون الارتباط غير موثوق به. بدلاً من ذلك، قم بزيارة مواقع ويب من خلال كتابة محدد موقع المعلومات (URL) الخاص بها في المستعرض أو استخدام ارتباط "المفضلة". لا تقم بنسخ ارتباطات ولصقها من رسائل في المستعرض .

استخدم كلمات مرور قوية وقم بتغييرها بشكل متكرر إذا كان الحساب الخاص بك يسمح بذلك، فاستخدم كلمات المرور القوية التي تجمع بين الأحرف الكبيرة والصغيرة

والأرقام والرموز، مما يجعل من الصعب على الآخرين تخمين كلمة المرور. لا تستخدم كلمات حقيقية. استخدم كلمة مرور مختلفة لكل حساب من حساباتك وقم بتغييرها بشكل متكرر. يصعب تذكر كل كلمات المرور هذه. للحصول على تلميحات عن إنشاء كلمات مرور قوية وكيفية تذكر كلمات المرور وتخزينها بأمان.

عدم إرسال معلومات شخصية في رسائل البريد الإلكتروني العادية رسائل البريد الإلكتروني العادية هي رسائل غير مشفرة، فهي تشبه إرسال البطاقات البريدية. إذا اضطررت إلى استخدام رسائل البريد الإلكتروني للمعاملات الشخصية، فاستخدم Outlookلكي يقوم بتوقيع الرسائل وتشفيرها رقمياً باستخدام أمان .S/MIME

يدعم كل من MSN® و Hotmail® و Outlook Expressو Microsoft Office Outlook Web Access و Lotus Notesو Netscape و Eudoraأمان .S/MIME

التعامل مع الشركات التي تعرفها وتثق بها فقط تعامل مع الشركات المعروفة والرسمية ذات السمعة الجيدة في جودة الخدمة. يجب أن يكون لدى موقع الأعمال على ويب بيان خصوصية يعلن تحديداً أنه لن يتم إبلاغ الآخرين عن اسمك أو المعلومات الخاصة بك .

التأكد من أن موقع ويب يستخدم التشفير يجب أن يسبق عنوان ويب بـ **https://**بدلاً من **http://** العادي في شريط العنوان الخاص بالمستعرض. كذلك، انقر نقراً مزدوجاً فوق رمز القفل على شريط معلومات المستعرض لعرض الشهادة الرقمية الخاصة بالموقع. يجب أن يتطابق الاسم الذي يلي **صادر لأجل** في الشهادة مع الموقع الذي تستخدمه. إذا ساورك الشك أن موقع ويب ليس هو الموقع المطلوب، قم بمغادرة الموقع في الحال وأبلغ عنه. لا تتَّبع أي إرشادات يقدمها هذا الموقع .

المساعدة على حماية الكمبيوتر الخاص بك من المهم استخدام جدار حماية والإبقاء على جهاز الكمبيوتر محدَّثاً واستخدام

البرامج المضادة للفيروسات، خاصة إذا كنت متصلاً بإنترنت من خلال مودم كبل أو مودم خط مشترك رقمي .(DSL) للحصول على معلومات عن كيفية القيام بذلك، قم بزيارة حماية الكمبيوتر،ينبغي أيضاً التفكير في استخدام البرامج المضادة للتجسس. يمكن تنزيل برامج Microsoft المضادة للتجسس أو استخدام منتج طرف ثالث يوفره موقع تنزيلات برامج الأمان والنسخ التجريبية الخاصة بها .

مراجعة المعاملات التي تجريها راجع تأكيدات الحوالات وبطاقة الائتمان وبيانات البنك بمجرد تلقيها للتأكد من أنك بصدد تسديد رسوم المعاملات التي أجريتها فقط. قم في الحال بالإبلاغ عن أي أمور غير عادية تراها في الحسابات الخاصة بك، وذلك بالاتصال بالرقم الموضح في بيان الحساب. يؤدي استخدام بطاقة ائتمان واحدة فقط للصفقات عبر إنترنت إلى سهولة تعقب المعاملات التي تجريها .

استخدام بطاقات الائتمان للمعاملات على إنترنت في معظم الإعدادات المحلية، تعتبر

مسؤوليتك الشخصية في حال قيام شخص ما بتعريض بطاقة الائتمان الخاصة بك لخطر السرقة محدودةً جدا. وبشكل معاكس، عند الصرف مباشرة من حساب البنك أو من بطاقة إيداع، فغالباً ما يتأثر رصيد حسابك المصرفي بأكمله .بالإضافة إلى ذلك، يفضل استخدام بطاقة الائتمان ذات حد ائتمان صغير على إنترنت لأنها تقيد كمية الأموال التي بإمكان اللص سرقتها عند تعرض البطاقة للخطر. وأفضل من ذلك، يوفر الآن العديد من الشركات المصدرة لبطاقات الائتمان للعملاء خدمة التسوق عبر إنترنت بأرقام بطاقات ائتمان افتراضية تستخدم مرةً واحدة، وهذه الأرقام تنتهي مدة صلاحيتها في غضون شهر أو شهرين. لمزيد من التفاصيل، راجع البنك الخاص بك في ما يتعلق بأرقام بطاقات الائتمان الافتراضية المحددة بمدة زمنية .

تلميحات عن التسوق والتعاملات البنكية بشكل آمن عبر الإنترنت

إذا أردت الحصول على معلومات إضافية من Microsoftعن الطرق التي تساعد في حماية المعلومات الشخصية أثناء التسوق أو التعاملات البنكية عبر الإنترنت، فقم بزيارة موقع الاحتيال عبر الإنترنت .ضع في الاعتبار أنه ليس كل سارقي الهويات متسللين ذوي كفاءة عالية. يستخدم البعض منهم أساليب بسيطة، مثل البحث في القمامة عن معلومات شخصية مهملة. قم بشراء أداة لتقطيع الأوراق المهملة والفواتير وعروض الائتمان مسبقة الاعتماد والمستندات الأخرى التي تحتوي على معلومات شخصية قبل إلقائها في سلة المهملات أو إعادة تدويرها.

الفهرس:

١٩- المعالج

٢٠-٢١-٢٢ شرح x p

٢٣-٢٤-٢٥

هل ألعاب الكمبيوتر تضيع وقت المعاق ذهنيا

٢٥-٢٦ تثير الحرارة على الجهاز

٢٧-٢٨-٢٩-٣٠- ٣١

لعبة الأطفال مع الكمبيوتر:

المحتالون

٣٢-٣٣-٣٤-٣٥-٣٦-٣٧-٣٨-٣٩-٤٠-٤١-٤٢-
٤٣-٤٤-٤٥-٤٦-٤٧-٤٨-٤٩-٥٠-٥١-٥٢